

CLAIM AMENDMENTS

Claims 1-9, 12, 13 and 15-23 are pending. Claims 10, 11 and 14 have been canceled. Claims 1, 12, 13 and 19 are amended herein. Claims 20-23 are newly added.

1 1 (currently amended): A fingerprint recognizing display system comprising:
2 a monitor having a screen and a front cover surrounding said screen;
3 a fingerprint recognizing module included with said monitor, said fingerprint recognizing
4 module including a fingerprint image recognizing unit disposed on a surface of said front cover,
5 wherein a user desiring access to said fingerprint recognizing display system touches said fingerprint
6 image recognizing unit; and
7 a computer main body including a fingerprint data base and a fingerprint verifying unit,
8 wherein said fingerprint verifying unit compares fingerprint data transmitted from said fingerprint
9 recognizing module to registered fingerprint data stored in said fingerprint data base and permits said
10 user access to programs stored in said fingerprint recognizing display system when it is determined
11 that the fingerprint of said user matches fingerprint data stored in said fingerprint data base, said
12 computer main body comprising:
13 a kernel of an operating system of said computer main body for determining whether
14 said fingerprint data base has been established in said computer main body; and
15 said kernel recognizing that said fingerprint recognizing display system has been
16 activated and performing a fingerprint registration routine when it is determined that said
17 fingerprint data base has not been established, and determining whether said monitor is a

18 fingerprint recognizing monitor when it is determined that said fingerprint data base has been
19 established.

1 2 (original): The fingerprint recognizing display system as set forth in claim 1, wherein said
2 fingerprint image recognizing unit is integrally formed with a power switch disposed on the surface
3 of said front cover.

1 3 (original): The fingerprint recognizing display system as set forth in claim 1, wherein said
2 fingerprint recognizing module also includes:

3 a converter converting analog fingerprint data input from the fingerprint image recognizing
4 unit to digital fingerprint data, and

5 a first communication unit transmitting the digital fingerprint data to a second
6 communication unit in the computer main body.

1 4 (original): The fingerprint recognizing display system as set forth in claim 1, wherein said
2 monitor includes a microprocessor communicating with a video card in said computer main body.

1 5 (original): The fingerprint recognizing display system as set forth in claim 4, wherein said
2 fingerprint recognizing module also includes:

3 a converter converting analog fingerprint data input from the fingerprint image recognizing
4 unit to digital fingerprint data, and

5 said microprocessor transmits the digital fingerprint data to a communication unit in the
6 computer main body.

1 6 (previously presented): The fingerprint recognizing display system as set forth in claim 1,
2 wherein said fingerprint verifying unit includes:

3 a decoding unit for decoding the registered fingerprint data read from said fingerprint data
4 base;

5 an encoding unit for encoding fingerprint data for storage into said fingerprint data base;

6 a distinctive feature detecting unit for detecting a distinctive feature of a fingerprint
7 corresponding to the fingerprint data transmitted from said monitor;

8 a fingerprint matching/recording unit for receiving decoded fingerprint data from said
9 decoding unit and also for providing fingerprint data to said encoding unit, said fingerprint
10 matching/recording unit comparing decoded fingerprint data received from said decoding unit to said
11 distinctive feature received from said distinctive feature detecting unit and also for outputting said
12 distinctive feature received from said distinctive feature detecting unit to said encoding unit to be
13 stored as the registered fingerprint data in said fingerprint data base; and

14 a recognizing unit outputting a "pass" signal or a "fail" signal in response to a comparison
15 result output from said fingerprint matching/recording unit.

1 7 (previously presented): The fingerprint recognizing display system as set forth in claim 3,
2 wherein said fingerprint verifying unit includes:

3 a decoding unit for decoding the registered fingerprint data read from said fingerprint data
4 base;

5 an encoding unit for encoding fingerprint data for storage into said fingerprint data base;

6 a distinctive feature detecting unit for detecting a distinctive feature of a fingerprint
7 corresponding to the fingerprint data transmitted from said first communication unit to said second
8 communication unit;

9 a fingerprint matching/recording unit for receiving decoded fingerprint data from said
10 decoding unit and also for providing fingerprint data to said encoding unit, said fingerprint
11 matching/recording unit comparing decoded fingerprint data received from said decoding unit to said
12 distinctive feature received from said distinctive feature detecting unit and also for outputting said
13 distinctive feature received from said distinctive feature detecting unit to said encoding unit to be
14 stored as the registered fingerprint data in said fingerprint data base; and

15 a recognizing unit outputting a "pass" signal or a "fail" signal in response to a comparison
16 result output from said fingerprint matching/recording unit.

1 8 (previously presented): The fingerprint recognizing display system as set forth in claim 5,
2 wherein said fingerprint verifying unit includes:

3 a decoding unit for decoding the registered fingerprint data read from said fingerprint data
4 base;

5 an encoding unit for encoding fingerprint data for storage into said fingerprint data base;

6 a distinctive feature detecting unit for detecting a distinctive feature of a fingerprint

7 corresponding to the fingerprint data transmitted from said microprocessor to said communication
8 unit;

9 a fingerprint matching/recording unit for receiving decoded fingerprint data from said
10 decoding unit and also for providing fingerprint data to said encoding unit, said fingerprint
11 matching/recording unit comparing decoded fingerprint data received from said decoding unit to said
12 distinctive feature received from said distinctive feature detecting unit and also for outputting said
13 distinctive feature received from said distinctive feature detecting unit to said encoding unit to be
14 stored as the registered fingerprint data in said fingerprint data base; and

15 a recognizing unit outputting a "pass" signal or a "fail" signal in response to a comparison
16 result output from said fingerprint matching/recording unit.

1 9 (original): The fingerprint recognizing display system as set forth in claim 1, wherein said
2 monitor comprises a cathode ray tube display apparatus or a liquid crystal display apparatus.

1 10 (canceled)

1 11 (canceled)

1 12.(currently amended): A method of recognizing a fingerprint to enable a user to operate a
2 computer system including a monitor and a computer main body, said method being embodied in
3 an operating system kernel mode and comprising the steps of:

4 determining whether a fingerprint data base has been established in said computer main body
5 prior;

6 performing a fingerprint registration routine when it is determined that said fingerprint data
7 base has not been established.

8 determining whether said monitor is a fingerprint recognizing monitor when it is determined
9 that said fingerprint data base has been established;

10 detecting a fingerprint of the user when said user touches a portion of a front cover
11 surrounding a display screen of [[a]] said monitor of said computer system;

12 transmitting fingerprint data corresponding to said fingerprint of said user, when detected,
13 from said monitor to [[a]] said computer main body of said computer system;

14 comparing the fingerprint data transmitted from said monitor to registered fingerprint data
15 output from [[a]] said fingerprint data base, ~~included~~ when said fingerprint data base has been
16 established in said computer main body; and

17 enabling said computer system to be operated by said user when said comparing step
18 indicates that there is a match between the fingerprint data transmitted from said monitor and the
19 registered fingerprint data output from said fingerprint data base, or disabling said computer system
20 to prevent operation by said user when said comparing step indicates that there is not a match
21 between the fingerprint data transmitted from said monitor and the registered fingerprint data output
22 from said fingerprint data base.

1 13 (original): The method as set forth in claim 12, further comprising steps of:

2 ~~determining whether said monitor is a fingerprint recognizing monitor, and~~

3 determining that said monitor is operating in an abnormal status and preventing said
4 computer system from being operated when it is determined that said monitor is not a fingerprint
5 recognizing monitor, or performing said step of detecting a fingerprint when it is determined that
6 said monitor is a fingerprint recognizing monitor.

1 14 (canceled)

1 15 (original): The method as set forth in claim 13, further comprising steps of:

2 determining whether a keyboard or a mouse of said computer system is operated by said user
3 during operation of a screen protection routine of said computer system; and

4 continuing to run a screen saver program when it is determined that neither said keyboard
5 nor said mouse have been operated, or performing said step of determining whether said monitor is
6 a fingerprint recognizing monitor when it is determined that one of said keyboard or said mouse have
7 been operated.

1 16 (original): The method as set forth in claim 15, further comprising a step of ending said
2 screen protection routine when said comparing step indicates that there is a match between the
3 fingerprint data transmitted from said monitor and the registered fingerprint data output from said
4 fingerprint data base, and then performing said step of enabling said computer system to be operated
5 by said user.

1 17 (original): The method as set forth in claim 12, wherein said comparing step includes steps
2 of:
3 checking said fingerprint data transmitted from said monitor and detecting distinctive features
4 thereof;
5 determining whether the detected distinctive features are of good quality; and
6 outputting an error message when it is determined that the detected distinctive features are
7 not of good quality and returning to said step of detecting a fingerprint of the user, or performing said
8 comparing step when it is determined that the detected distinctive features are of good quality.

1 18 (previously presented): The method as set forth in claim 13, further comprising steps of:
2 determining whether a file stored in said computer system is enabled to be encoded or
3 decoded during operation of a file encoding/decoding routine of said computer system;
4 outputting an message indicating said file can not be encoded or decoded when it is
5 determined said file is not enabled to be encoded or decoded;
6 performing said step of determining whether said monitor is a fingerprint recognizing
7 monitor when it is determined said file is enabled to be encoded or decoded; and
8 permitting said user to encode or decode said file when said comparing step indicates that
9 there is a match between the fingerprint data transmitted from said monitor and the registered
10 fingerprint data output from said fingerprint data base.

1 19 (currently amended): The method as set forth in claim [[14]] 12, wherein said fingerprint
2 registration routine comprises the steps of:

3 detecting a fingerprint of a manager when said manager touches the portion of the front cover
4 of said monitor of said computer system;

5 transmitting fingerprint data corresponding to said fingerprint of said manager, when
6 detected, from said monitor to said computer main body of said computer system;

7 comparing the fingerprint data transmitted from said monitor to registered fingerprint data
8 output from a fingerprint data base included in said computer main body; and

9 permitting said manager to operate a fingerprint managing and registering program when said
10 comparing step indicates that there is a match between the fingerprint data transmitted from said
11 monitor and the registered fingerprint data output from said fingerprint data base, or disabling said
12 computer system to prevent operation by said manager when said comparing step indicates that there
13 is not a match between the fingerprint data transmitted from said monitor and the registered
14 fingerprint data output from said fingerprint data base.

1 20 (new): A method of recognizing a fingerprint to enable a user to operate a computer
2 system including a monitor and a computer main body, said method being embodied in a kernel of
3 an operating system of said computer main body and comprising the steps of:

4 determining whether a fingerprint data base has been established in said computer main body
5 prior;

6 performing a fingerprint registration routine when it is determined that said fingerprint data

7 base has not been established; and

8 determining whether said monitor is a fingerprint recognizing monitor when it is determined
9 that said fingerprint data base has been established.

1 21 (new): The method as set forth in claim 20, wherein said fingerprint registration routine
2 comprises the steps of:

3 detecting a fingerprint of a manager when said manager touches the portion of the front cover
4 of said monitor of said computer system;

5 transmitting fingerprint data corresponding to said fingerprint of said manager, when
6 detected, from said monitor to said computer main body of said computer system;

7 comparing the fingerprint data transmitted from said monitor to registered fingerprint data
8 output from a fingerprint data base included in said computer main body; and

9 permitting said manager to operate a fingerprint managing and registering program when said
10 comparing step indicates that there is a match between the fingerprint data transmitted from said
11 monitor and the registered fingerprint data output from said fingerprint data base, or disabling said
12 computer system to prevent operation by said manager when said comparing step indicates that there
13 is not a match between the fingerprint data transmitted from said monitor and the registered
14 fingerprint data output from said fingerprint data base.

1 22 (new): The method as set forth in claim 20, further comprising steps of:

2 detecting a fingerprint of the user when said user touches a portion of a front cover

3 surrounding a display screen of said monitor of said computer system;

4 transmitting fingerprint data corresponding to said fingerprint of said user, when detected,
5 from said monitor to said computer main body of said computer system;

6 comparing the fingerprint data transmitted from said monitor to registered fingerprint data
7 output from said fingerprint data base, when said fingerprint data base has been established in said
8 computer main body; and

9 enabling said computer system to be operated by said user when said comparing step
10 indicates that there is a match between the fingerprint data transmitted from said monitor and the
11 registered fingerprint data output from said fingerprint data base, or disabling said computer system
12 to prevent operation by said user when said comparing step indicates that there is not a match
13 between the fingerprint data transmitted from said monitor and the registered fingerprint data output
14 from said fingerprint data base.

1 23 (new): The method as set forth in claim 20, further comprising steps of:

2 determining that said monitor is operating in an abnormal status and preventing said
3 computer system from being operated when it is determined that said monitor is not a fingerprint
4 recognizing monitor, or performing said step of detecting a fingerprint when it is determined that
5 said monitor is a fingerprint recognizing monitor.